KOREAN INTELLECTUAL PROPERTY OFFICE

KOREAN PATENT ABSTRACTS

(11)Publication number: 1020000062153 A

(43)Date of publication of application:

25.10.2000

(21)Application number: 1019990049429

(22)Date of filing: 09.11.1999

(30)Priority: 09.11.1998 1

(71)Applicant: LUCENT TECHNOLOGIES INC

(72)Inventor: BERENZWEIG ADAM L
BRATHWAITE CARLOS ENRIQUE

(51)Int. Cl H04B 7/26

(54) AUTHENTICATION METHOD BY UPDATED KEY

(57) Abstract:

PURPOSE: To obtain an efficient authentication execution method that uses an authentication call sent to a terminal so as to supply information about the authentication, and to calculate an encryption key to the terminal. CONSTITUTION: A visiting authentication center obtains a random number RT, an authentication key KA, and an encryption key KC from a host authentication center. The visiting authentication center transmits a random number RT to a transmitter to update an authentication key and an encryption key of the terminal and calls the terminal as a part of an authentication process. The terminal calculates the authentication key KA and the encryption key KC by using the RT and replies the call from the visiting authentication center. In addition, a reply of a visiting network to the authentication call of the terminal to the network is checked by using the authentication key.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) Int. Cl.[7]
H04B 7/26

(11) 공개번호 특2000-0062153
(43) 공개일자 2000년10월25일

(21) 출원번호 10-1999-0049429
(22) 출원일자 1999년11월09일
(30) 우선권주장 9/188818 1998년11월09일 미국(US)
(71) 출원인 루센트 테크놀러지스 인크
미합중국 뉴저지 머레이 힐 마운틴 애비뉴 600 (우편번호 : 07974-0636)
(72) 발명자 베렌즈위그,아담엘.
미국,뉴욕10003,뉴욕,#12-0,이스트12번스트리스70
브라스와이트,카롤엔리큐
미국,뉴저지07050,오렌지,힐러스트리트63
(74) 대리인 이병호

심사청구 : 없음

(54) 키 업데이트를 사용한 유효한 보증

요약

보증을 수행하는 더 유효한 방법이 보증 및 암호 키 값들을 계산하는 정보를 터미널에 제공하도록 터미널에 전송된 보증 챌린지를 사용함에 의해 제공된다. 결과적으로, 분리 통신은 터미널에 키 값들을 제공할 필요가 없다. 방문 보증 센터는 홈 보증 센터로부터 랜덤 값 R_T, 보증 키 값 K_A, 암호 키 값 K_C를 얻는다. 방문 보증 센터는 그 다음에 터미널의 보증 키 및 암호 키 값들을 업데이트하도록 터미널에 난수 R_T를 제공하고, 보증 과정의 부분으로 상기 터미널에 챌린지한다. 터미널은 보증 키 값 K_A과 암호 키 값 K_C을 계산하도록, 방문 보증 센터의 챌린지에 응답하도록 R_T를 사용한다. 부가적으로, 보증 키 값은 네트워크의 터미널의 보증 챌린지에 대한 방문 네트워크의 응답을 입증하는데 사용된다.

대표도

도5

색인어

기지국, 이동체, 홈 위치 레지스터, 방문 네트워크, 전화 번호, 홈 보증 센터

명세서

도면의 간단한 설명

도1은 이동체, 방문 네트워크, 홈 네트워크사이의 통신을 도시한 도면.

도2는 GSM 네트워크의 보증 처리를 도시한 도면.

도3a과 도3b는 IS41 컴플라이언트(compliant)네트워크의 키 업데이트 및 보증 처리를 도시한 도면.

도4는 제안된 상호 보증 방법을 도시한 도면.

도5는 키 업데이트들과 상호 보증을 수행하는 방법을 도시한 도면.

※도면의 주요부분에 대한 부호의 설명※

10 ; 기지국 14 : 이동체

발명의 상세한 설명

발명의 목적

발명이 속하는 기술분야 및 그 분야의 종래기술

발명의 분야

본 발명은 통신들에 관한 것이며, 특히 무선 통신 시스템들에서 통신 당사자(party)들의 보증에 관한 것

이다.

관련 기술의 설명

도1은 기지국(10), 그것과 연관된 셀(12), 셀(12)내의 이동체(mobile)(14)를 도시한다. 첫째로 이동체(14)가 기지국(10)과의 통신들을 등록하거나 시도하려할 때, 기지국(10)은 이동체로 하여금 통신 네트워크에 접속을 허용하기전에 이동체의 신원(identity)을 보증하거나 입증한다. 이동체(14)가 홈 네크워크 이외의 어떤 네트워크에 존재할 때, 이는 방문(visiting) 네크워크에 존재하는 것으로 언급된다. 홈 네크워크는 무선 통신 서비스들을 제공하도록 이동 터미널의 소유자와 계약한 서비스 제공자에 의해 제어되는 네트워트이다. 만일 이동체가 방문 통신 네트워크내에서 동작한다면, 기지국(10)에 의한 이동체의 보증은 이동체의 홈 네트워크의 보증 센터(16)와의 통신을 수반한다. 도1의 예에서, 이동체(14)는 방문 네트워크내에 존재한다. 결과적으로, 이동체(14)의 보증은 이동체의 홈 네트워크의 보증 센터(16)와의 통신을 수반한다. 이동체(14)가 방문자 네트워크에 접근하려 할 때, 기지국(10)은 방문 통신 네트워크의 보증 센터(18)와 통신한다. 보증 센터(18)는 이동체(14)가 홈 보증 센터(16)를 사용한 네트워크를 사용하여 등록됨을 이동체(14)의 전화 번호와 같은 이동체 또는 터미널 식별자로부터 결정한다. 방문 보증 센터(18)는 그 다음에 IS41신호 네트워크(20)와 같은 네트워트를 통해 홈 보증 센터(16)와 통신한다. 홈 보증 센터(16)는 그 다음에 이동체(14)의 등록 기재사항을 가지는 홈 위치 레지스터(22)에 접근한다. 홈 위치 레지스터(22)는 이동체의 전화 번호와 같은 식별자에 의해 터미널 또는 이동체와 연관될 수 있다. 홈 위치 레지스터에 포함된 정보는 암호 키들을 발생시키도록 사용되며, 다른 정보는 방문자 보증 센터(18)의 방문자 위치 레지스터(24)에 그 다음에 공급된다. 방문자 위치 레지스터(24)로부터의 정보는 그 다음에 이동체(14)가 응답하여 통신 서비스들을 받을 자격이 부여된 이동체로서 보증되도록 이동체(14)에 전송된 정보를 기지국(14)에 공급하도록 사용된다.

도2는 GSM 무선 네트워크들내에 사용되는 보증 절차를 도시한다. 이 경우, 이동체 및 홈 위치 레지스터는 키 Ki를 포함한다. 이동체가 방문 네트워크에 접근을 요청할 때, 방문 보증 센터는 RAND,SRES,Kc라는 변수들을 수신하도록 홈 보증 센터와 접촉한다. 홈보증 센터는 SRES,Kc라는 변수 값들을 발생시키도록 이동체와 연관된 홈 위치 레지스터로부터 킷값 Ki를 사용한다. SRES라는 값은 입력으로 난수(random number) RAND와 키 입력으로 Ki값을 가진 A3로 알려진 암호 함수를 사용하여 계산된다. 유사한 방법으로, 암호 키 Kc는 입력으로 RAND와 키 입력으로 Ki 값을 가진 암호 함수 A8를 사용함에 의해 계산된다. 이 값들은 방문 보증 센터의 방문자 위치 레지스터로 그 다음에 전송된다. 방문 보증 센터는 그 다음에 이동체에 난수 RAND를 전송함에 의해 이동체를 챌린지(challenge)한다. 이동체는 그 다음에 홈 보증 센터에 의해 계산되는 방법과 같은 방법으로 SRES,Kc라는 값들을 계산한다. 이동체는 그 다음에 방문 보증 센터에 SRES라는 값을 전송하며, 여기서 방문 보증 센터는 이동체로부터 수신된 변수 SRES와 홈 보증 센터로부터 수신된 변수 SRES를 비교한다. 만일 이 값들이 일치하면, 이동체는 방문 네트워크에 접근이 허용된다. 만일 이동체와 방문 네트워크사이의 추가적인 통신들이 암호화된다면, 이들은 입력으로 암호화된 메시지와, 변수 값 Kc와 같은 키 입력을 가진 암호 함수 A5를 사용하여 암호화된다. A3,A5,A8이라는 암호 함수들은 상기 기술에 잘 알려져 있고, GSM 표준에 의해 권고된다. GSM 시스템에 있어서, 홈 보증 센터와의 통신을 포함하는 이 보증 처리는 이동체가 방문 네트워크와 새로운 호출을 개시할 때마다 수행된다.

도 3a와 도3b는 IS41 컴플라이언트(compliant)네트워크에 사용되는 보증 과정을 도시한다. IS41 컴플라이언트 네트워크들의 예들은 AMPS,TDMA,CDMA 프로토콜들을 사용하는 네트워크들이다. 이 시스템에서, 이동체 와 홈 위치 레지스터는 AKEY라고 불리는 비밀 값을 포함한다. 이동체가 방문 네트워크에 접근을 요청할 때, 방문 네트워크 보증 센터는 홈 보증 센터로부터 데이터를 요청한다. 실제 보증 처리가 개시되기 전에, 키 업데이트(update)는 보증 및 통신의 암호 알고리즘들로 사용되는 키들을 이동체와 방문 위치 레지스터에 제공함에 의해 수행된다. 이동체와 연관된 홈 위치 레지스터가 위치되며, 이동체의 전화 번호와 같은 식별자를 사용하고, 홈 위치 레지스터내에 기억된 AKEY 값은 방문자 위치 레지스터에 전송되는 데이터를 발생시키기 위해 사용된다. 계산된 값들은 SSDA(shared Secret Data A),SSDB(Shared Secret Data B)값들이다. 이 값들은 입력으로 난수 RS와 키 입력으로 AKEY 값을 사용한 CAVE 알고리즘을 수행함에 의해 계산된다. 이 CAVE 알고리즘은 상기 기술에 잘 알려져 있고, IS41 표준에서 상술된다. 홈 보증 센터는 그 다음에 방문 네트워크의 방문자 위치 레지스터에 Rs,SSDA,SSDB라는 값들을 전송한다. 방문 네트워크는 그 다음에 이동체에 Rs를 전송함으로써 상기 이동체에 의해 사용되는 SSDA,SSDB(shared secret data)를 업데이트한다. 이동체는 그 다음에 홈 보증 센터에 의해 계산되는 방법과 같은 방법으로 SSDA,SSDB를 계산한다. 이제 이동체와 방문자 위치 레지스터가 SSDA,SSDB 값들을 포함하므로, 보증 처리가 발생하게 된다.

도3b는 이동체와 방문 위치 레지스터가 SSDA,SSDB라는 키 값들을 수신한 후에 방문 네트워크내에서 이동체가 어떻게 보증되는 지를 도시한다. 방문 보증 센터는 이동체에 난수 R_N 을 전송함에 의해 이동체를 챌린지한다. 이 때, 이동체와 방문 보증 센터는 AUTHR 라는 값을 계산하며, 여기서 값 AUTHR은 입력으로 난수 R_N 과, 키 입력으로 SSDA 값을 사용한 CAVE 알고리즘의 출력과 같다. 이동체는 그 다음에 방문 보증 센터에 계산된 값 AUTHR 을 전송한다. 방문 보증 센터는 AUTHER인 계산된 값과 이동체로부터 수신된 값을 비교한다. 만일 이 값들이 일치하면, 이동체는 보증되고, 방문 네트워크에 접근이 허용된다. 부가적으로, 이동체와 방문 보증 센터는 암호 키 값 Kc 을 계산하며, 여기서 Kc라는 값은 입력으로 값 R_N 과, 키 입력으로 값 SSDS를 사용한 CAVE 알고리즘의 출력과 같다. 이 때, 이동체와 방문 네트워크사이의 통신들이 허용되고, 암호 함수를 사용하여 암호화될 수 있으며, 여기서 입력들은 암호화된 메시지와 Kc라는 키 값이다. 암호 함수들은 CDMA,TDMA 의 각각의 표준들에 의해 상술된다. IS41에 대하여, 방문 보증 센터와 홈 보증 센터사이의 통신들은 호출이 이동체에 행해질 때 마다와는 반대로, 단지 이동체가 방문 네트워크를 사용하여 등록할 때 마다 수행됨을 주목해야 한다.

상술된 방법들은 이동체가 네트워크에 접근하도록 허용됨을 입증하는 방법을 도시하며, 상기 방법들은 이동체가 정통적인(legitimate) 네트워크에 의해 자신을 식별하도록 요청됨을 입증하는 이동체는 취급하지 않는다. 도4는 방문 네트워크와 이동체사이의 상호 보증을 허용하는 IS41표준의 향상된 제안 사항을 도시한다. 도4는 일단 이동체와 방문 위치 레지스터가 도3a에서 상술된 SSDA,SSDB 값들을 수신하는 상호

보증 처리를 도시한다. 방문 네트워크는 난수 R_N 를 전송함에 의해 이동체를 챌린지 한다. 이동체는 그 다음에 입력들로 R_N,R_M 값들과, 키입력으로 SSDA 값을 사용하는 암호 함수 F^1 의 출력을 얻기위한 계산을 수행함에 의해 응답한다. 이 경우, R_N 값은 방문 네트워크에 의해 전송된 같은 값이고, R_M 값은 이동체에 의해 계산된 난수이다. 이 암호 함수의 출력을 전송함에 더하여, R_M 값은 방문 네트워크에 비암호화된 형식으로 또한 전송된다. 방문 네트워크는 키 입력으로 SSDA 값을 사용하는 F^1 암호 함수에 입력들로, R_N 값들과 R_M의 비암호화된 형태를 사용하는 암호 함수 F^1 의 출력을 계산한다. 이 출력 값은 이동체로부터 수신된 값과 비교되며, 만일 이들 값들이 일치하면, 이동체는 입증되거나 보증된다. 방문 네트워크는 그 다음에 R_M 값의 형태로 이동체에 의해 제공된 챌린지(통신)에 응답함으로써, 이동체에 의해 보증되거나 입증된다. 방문 보증 센터는 그 다음에 입력으로 R_M 값과, 키 입력으로 SSDA 값을 사용하는 암호 함수 F^2 의 출력을 전송한다. 이동체는 그 다음에 같은 계산을 수행하고, 방문 네트워크로부터 수신된 값과, 키 값 SSDA 와 R_M 값을 사용하는 암호 함수 F^2 의 출력으로부터 얻어진 값을 비교한다. 만일 이 값들이 일치하면, 이동체는 네트워크가 보증되거나 입증되었다고 간주하며, 네트워크와의 통신을 계속한다. 방문 보증 센터와 이동체 양쪽은 입력들로 R_N,R_M 과, 키 입력으로 SSDB 값을 사용하는 암호 함수 F^3 의 출력을 얻음에 의해 암호 키 Kc의 값을 계산한다. 이 때, 이동체와 방문 네트워크는 통신할 수 있다.; 그러나, 만일 암호화된 통신들이 소망되면, 메시지들은 입력으로 암호화된 메시지와, 키 입력으로 Kc 값을 가진 암호 알고리즘 F^4 를 사용하여 암호화된다. 암호 함수들 F^1,F^2,F^3는 해시(hash) 함수들이거나 SHA-1와 같은 하나의 암호 함수일 수 있으며, 함수 F^4 는 DES와 같은 암호 함수일 수 있다. 해시 함수들과, SHA-1과 같은 암호 함수들과 DES와 같은 암호 함수들은 상기 기술에 잘 알려져 있다.

발명이 이루고자 하는 기술적 과제

제안된 상호 보증 처리는 이동체와 방문 위치 레지스터가 보증 처리를 개시하기 전에 SSDA,SSDB 값들을 가져야 한다는 점에서 비효율성을 갖는다. 결과적으로 , 적어도 2개 세트의 통신은 이동체와 방문 보증 센터사이에서 요구된다. 제1 세트의 통신은 SSDA,SSDB 값들을 계산하도록 사용된 정보를 이동체에게 제공한다. 제2 세트의 통신은 상호 보증을 수행하도록 사용된다.

발명의 구성 및 작용

발명의 개요

본 발명은 터미널에 보증 및 암호 키 값들을 계산하는 정보를 제공하도록 터미널에 전송된 보증 챌린지를 사용함에 의해 보증처리를 수행하는 더 유효한 방법을 제공한다. 결과적으로, 분리 통신은 터미널에 키 값들을 제공할 필요가 없고, 2개 세트의 통신의 비효율성이 제거된다. 방문 보증 센터는 홈 보증 센터로부터 랜덤 값 R_T 보증키 값 K_A, 암호 키 값 Kc을 얻는다. 방문 보증 센터는 그 다음에 터미널의 보증 키와 암호 키 값들을 업데이트하도록 터미널에 난수 R_T 를 전송하며, 보증 처리의 부분으로 터미널을 챌린지한다. 터미널은 보증 키 값 K_A 과 암호 키 값 Kc를 계산하도록, 방문 보증 센터의 통신에 응답하도록 R_T 값을 사용한다. 부가적으로. 보증 키 값은 네트워크의 터미널 보증 챌린지에 방문 네트워크의 응답을 입증하도록 사용된다.

상세한 설명

도5는 이동체 또는 정지 터미널에 전송된 단일 랜덤 값이 터미널의 보증 및 암호 키 값들을 업데이트하도록, 터미널에 보증 챌린지를 제공하도록 사용되는 방법을 도시한다. 이동 또는 정지 터미널(70), 홈 위치 레지스터(72)는 키 값 Ki를 분배한다. 이동 터미널(70)이 방문 네트워크에 접근을 요청할 때, 방문 보증 센터는 랜덤 값 R_T, 보증 키 값 K_A, 암호 키 값 Kc을 얻기 위해 홈 보증 센터와 접촉한다. 이 요청에 응답하여, 홈 보증 센터는 방문 보증 센터를 통해 이동 터미널에 의해 제공된 전화 번호와 같은 식별자를 사용하여 이동 터미널(70)과 연관된 홈 위치 레지스터(72)에 접근한다. 홈 보증 센터는 그 다음에 입력으로 난수 R_T와, 키 입력으로 값 Ki를 사용하여 암호 함수 F^A 의 출력을 가짐에 의해 보증 키 값 K_A을 계산한다. 부가적으로, 홈 보증 센터는 입력으로 값 R_T와, 키 입력으로 값 Ki를 사용하는, 암호 함수 F^C 의 출력을 사용하여 암호 키 값 K_C 를 계산한다. 일단 이 값들이 계산되면, 홈 보증 센터는 방문 보증 센터와 R_T,K_A,K_C 값들을 통신한다. 방문 보증 센터는 그 다음에 이동 터미널(70)과 연관된 방문 위치 레지스터내에 KA,K_C,R_T 값들을 기억한다. 방문 보증 센터는 그 다음에 이동 터미널에 의해 사용된 보증 및 암호 키 값들을 업데이트 하도록 사용되는 값 및 보증 챌린지로, 이동 터미널(70)과 R_T 값을 통신한다. 이동 터미널은 값들이 홈 보증 센터에 의해 계산되는 방법과 같은 방법으로, 보증 키 값 K_A 과 암호 키 값 K_C 을 계산하도록 방문 보증 센터로부터 수신된 값 R_T 사용한다. 이동 터미널은 그 다음에 방문 보증 센터의 보증 챌린지에 응답하도록 보증 키 값 K_A를 사용한다. 이동 터미널은 입력들로 R_T,R_M 값들과, 키 입력으로 보증 키 값 K_A를 사용하여, 암호 함수 F^1의 출력을 결정한다.; 그러나, 입력들로 R_T,R_M보다 R_T 값을 또한 사용할 수 있다. 암호 함수 F^1 의 출력과 값 R_T는 방문 보증 센터와 통신한다.; 그러나 만일 R_M이 암호 함수 F^1의 입력으로 사용되지 않거나 네트워크의 보증이 필요치 않으면 값 R_M 은 전송되지 않을 수 있다.

값 R_M 은 이동 터미널에 의해 선택된 랜덤 값이다. 방문 보증 센터는 결과 값이 이동 터미널에 의해 통신된 값과 비교될 수 있도록, 입력들 R_T,R_M 과, 키 입력 값 K_A을 사용하는 함수 F^1의 출력 값을 또한 계산한다. 만일 이 값들이 일치하면, 이동 터미널은 그 다음에 방문 네트워크에 대해 보증되거나 입증된다. 이동 터미널에 의해 제공된 R_M 값은 이동체(70)에 의한 방문 네트워크에 보증 챌린지로서 사용된다. 이동체(70)에 의해 방문 네트워크에 보증 통신으로 사용된다. 방문 네트워크는 입력으로 값 R_M 과, 키 입력으로 값 K_A를 사용하는, 함수 F^2 의 출력을 계산한다. 이 출력 값은 그 다음에 이동 터미널과 통신하며, 여기서 상기 터미널은 독립적으로 입력으로 값 R_M 과, 키 입력으로 값 K_A 를 사용한 함수 F^2의 출력을 결정한다. 만일 출력 값들이 일치하면, 이동 터미널은 그 다음에 방문 네트워크에서 입증하거나 보증한다.

발명의 효과

일단, 이동 터미널과 방문 네트워크가 서로의 식별자들에 의해 보증되거나 입증되면, 통신은 계속된다. 통신은 비암호화된 메시지들 또는 암호화된 메시지들을 사용하여 이루어질수 있다. 만일 암호화된 메시지들이 사용되면, 상기 메시지들은 입력으로 메시지와, 키 입력으로 암호 값 K_C 을 사용하는, 암호 함수 F^2의 출력을 사용함에 의해 암호화된다. 이 처리는 이동 터미널 및 방문 네트워크사이에 호출이 시도될 때 마다 수행될 수 있다. 매번 호출이 시도될 때의 경우 보다 매번 이동체가 방문 네트워크를 사용하여 등록할 때의 경우에 홈 보증 센터와 또한 접촉가능하며, 이동체가 방문 네트워크를 사용하여 등록되어 남아 있는 한 같은 값들 K_A,K_C,R_T을 사용할 수 있다. 암호 함수들 F^1,F^2,F^A,F^C 는 하시 함수들이거나 SHA-1과 같은 하나의 암호 함수일 수 있으며, 함수 F^3는 DES와 같은 암호 함수일 수 있다. 하시 함수들과, SHA-1와 같은 암호 함수들 및 DES와 같은 암호 함수들은 상기 기술에 잘 알려져 있다.

이동 터미널이 홈 네트워크내에 존재 할 때, 같은 절차를 수행할 수 있다. 이 경우에, 방문 보증 센터보다 홈 보증 센터는 이동 터미널과 통신한다. 무선 네트워크에서, 터미널과 보증 센터사이의 통신들은 무선 베이스 기지국을 통해 이루어 진다.

(57) 청구의 범위

청구항 1

보증 방법에 있어서,

터미널에 제1 값을 전송하는 단계와,

적어도 제1 응답 값을 가지는 상기 터미널로부터 응답을 수신하는 단계로서, 상기 제1 응답 값은 적어도 입력으로 상기 제1 값과, 키 입력으로 제1 키 값안 제1 부분을 사용하는 적어도 제1 암호 함수의 출력의 부분이며, 상기 제1 키 값은 적어도 입력으로 상기 제 1 값과 키 입력으로 제 2 키 값인 제2 부분을 사용하는 제 2 암호 함수의 출력의 부분인 수신하는 단계와,

상기 제1 응답 값은 예기된 제1 응답 값과 같음을 입증하는 단계를 포함하는, 보증 방법.

청구항 2

제1항에 있어서, 상기 제2 키 값은 상기 터미널과 연관되는, 보증 방법.

청구항 3

제1항에 있어서, 상기 제1 및 제2 암호 함수들은 같은, 보증 방법.

청구항 4

제1항에 있어서, 상기 제1 및 제2 부분들은 같은, 보증 방법.

청구항 5

제1항에 있어서, 상기 응답은 제2 응답 값을 가지며, 상기 터미널에 제2 값을 전송하는 상기 단계를 더 포함하며, 상기 제2값은 적어도 입력으로 상기 제2 응답 값과, 키 입력으로 제3 키 값인 부분을 사용하는 적어도 제3 암호 함수의 출력의 부분인, 보증 방법.

청구항 6

보증 방법에 있어서,

터미널에 제1 값을 전송하는 단계와,

적어도 제1 응답 값 및 제2 응답 값을 가지는 상기 터미널로 부터 응답을 수신하는 단계로서, 상기 제 1 응답 값은 적어도 상기 제1 값의 제1 부분을 사용한 적어도 제1 암호 함수의 출력의 부분 및, 적어도 입력들로 상기 제2 응답 값과 키 입력으로 제1 키 값의 제1 부분이며, 상기 제1 키 값은 적어도 입력으로 상기 제 1 값과, 키 입력으로 제2 키 값의 제2 부분을 사용한 적어도 제2 암호 함수의 출력의 부분인 수신단계와,

상기 제1 응답 값은 예기된 제1 응답 값과 같음을 입증하는 단계를, 포함하는, 보증 방법.

청구항 7

제6항에 있어서, 상기 제2 키 값은 상기 터미널과 연관된, 보증 방법.

청구항 8

제6항에 있어서, 상기 제1 및 제2 암호 함수들은 같은, 보증 방법.

청구항 9

제6항에 있어서, 상기 제 1 값의 제1 및 제2 부분들은 같은, 보증 방법.

청구항 10

제6항에 있어서, 상기 터미널에 제2 값을 전송하는 상기 단계로서, 상기 제2 값은 적어도 입력으로 상기 제2 응답 값과 키 입력으로 제3 키 값의 제2 부분을 사용한 적어도 제3 암호 함수의 출력의 부분인, 보증 방법.

청구항 11

보증 방법에 있어서,

제1값을 수신하는 단계와,

적어도 제1 응답 값을 가지는 응답을 전송하는 단계로서, 상기 제1 응답값은 적어도 입력으로 상기 제1 값과 키 입력으로 제1 키 값인 제 1 부분을 사용한 적어도 제1 암호 함수의 출력의 부분이며, 상기 키 값은 적어도 입력으로 상기 제1 값과 키 입력으로 제 2 키 값인 제 2 부분을 사용한 적어도 제2 암호 함수의 출력의 부분인 전송 단계를 포함하는, 보증 방법.

청구항 12

제11항에 있어서, 상기 제1 및 제2 암호 함수들은 같은, 보증 방법.

청구항 13

제11항에 있어서, 상기 제1 및 제2 부분들은 같은, 보증 방법.

청구항 14

제11항에 있어서, 상기 응답은 제2 응답값을 가지며, 제2 값을 수신하는 상기 단계를 더 포함하며, 상기 제2 값은 적어도 입력으로 상기 제2 응답 값과 키 입력으로 제3 키 값인 부분을 사용한 적어도 제3 암호 함수의 출력의 부분인, 보증 방법.

청구항 15

제14항에 있어서, 상기 제 2 값이 예기된 제2 값과 같음을 입증하는 상기 단계를 더 포함하는, 보증 방법.

청구항 16

보증 방법에 있어서,

제1값을 수신하는 단계와,

적어도 제1 응답 값과 제2 응답 값을 가지는 응답을 전송하는 단계로서, 상기 제1 응답값은 적어도 제1 값의 제1 부분 및 적어도 입력들로 상기 제2 응답 값과 키 입력으로 제1 키 값인 제 1 부분을 사용한 적어도 제1 암호 함수의 출력의 부분이며, 상기 제1 키값은 적어도 입력으로 상기 제1 값과 키 입력으로 제2 키 값인 제 2 부분을 사용한 적어도 제2 암호 함수의 출력의 부분인 전송 단계를 포함하는, 보증 방법.

청구항 17

제16항에 있어서, 상기 제1 및 제2 암호 함수들은 같은, 보증 방법.

청구항 18

제16항에 있어서, 상기 제1 값의 상기 제1 및 제2 부분들은 같은, 보증 방법.

청구항 19

제16항에 있어서, 제2 값을 수신하는 상기 단계로서, 상기 제2 값은 적어도 입력으로 상기 제2 응답 값과 키 입력으로 제3 키 값의 제2 부분을 사용한 적어도 제3 암호 함수의 출력의 부분인 상기 단계를 더 포함하는, 보증 방법.

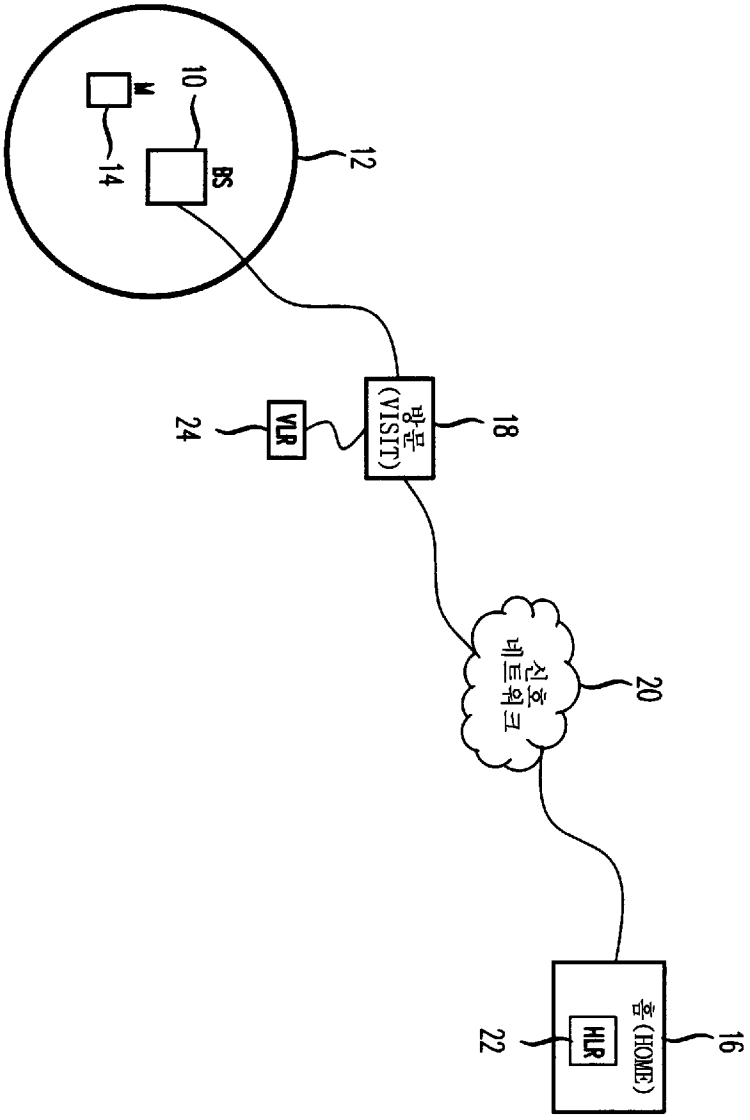
청구항 20

상기 제 2 값은 예기된 제2 값과 같음을 입증하는 상기 단계를 더 포함하는, 보증 방법.

도면

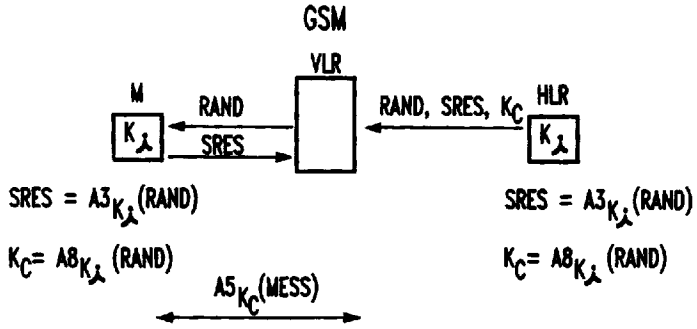
도면1

종래기술



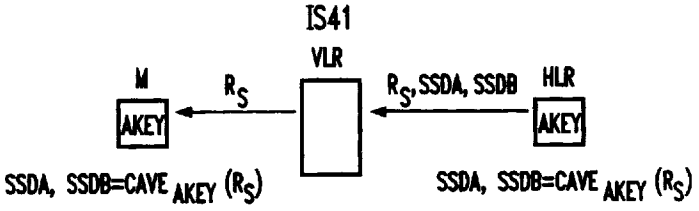
도면2

종래기술



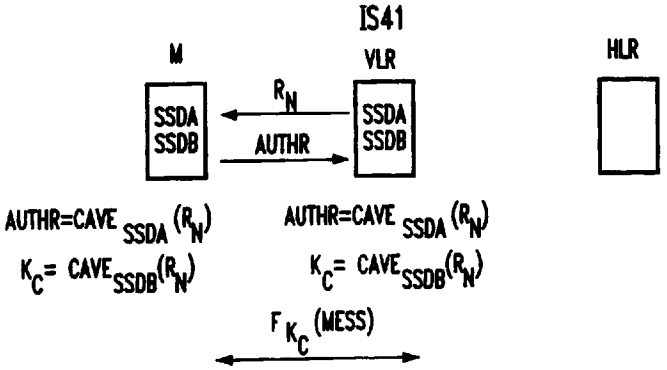
도면3a

종래기술



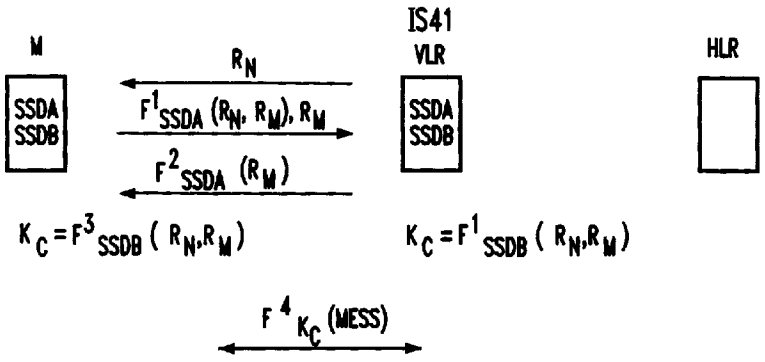
도면3b

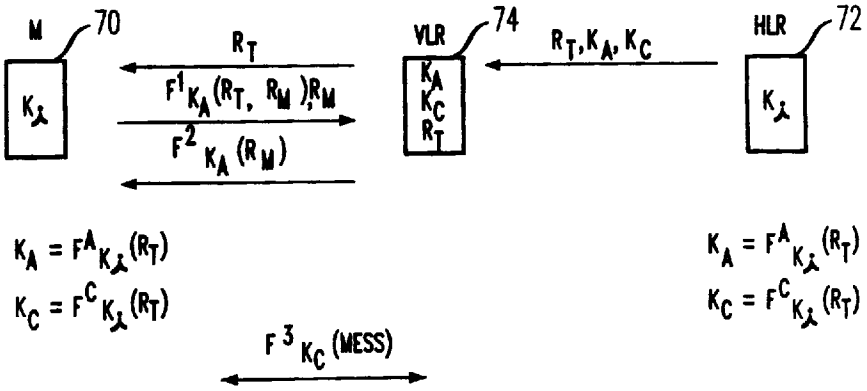
종래기술



도면4

종래기술




M
70
K_i
R_T
$F^1K_A(R_T, R_M), R_M$
$F^2K_A(R_M)$
VLR
74
K_A
K_C
R_T
R_T, K_A, K_C
HLR
72
K_i
$K_A = F^A K_i(R_T)$
$K_C = F^C K_i(R_T)$
$K_A = F^A K_i(R_T)$
$K_C = F^C K_i(R_T)$
$F^3 K_C$ (MESS)